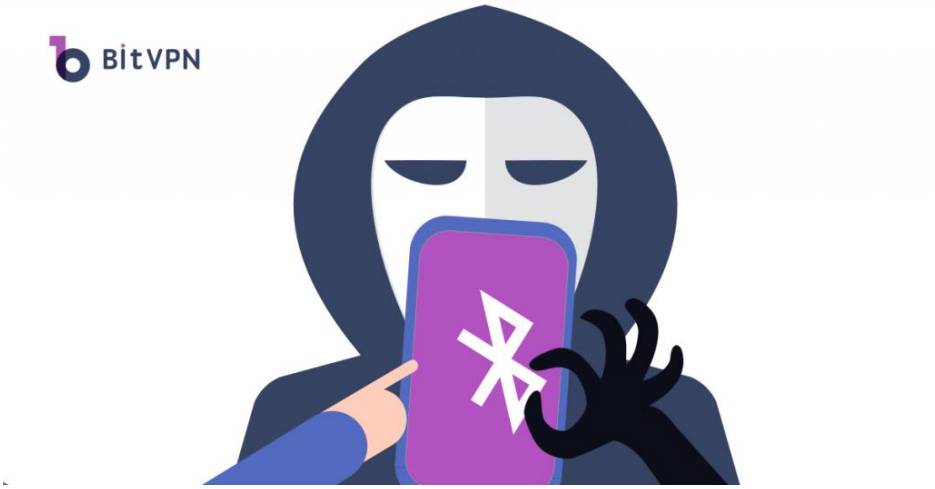
Can My Phone be Hacked through Bluetooth by Someone?

by Joe Zahl

Bluetooth technology is built into all cell phones and other devices. Bluetooth connection allows quick and easy connection of phones with headphones, speakers, TVs, and other devices with Bluetooth technology built-in. However, do you know that sometimes it's Bluetooth that may expose your phone to being hacked by someone?

Bluetooth hacks can take place when a hacker uses their own Bluetooth connection to gain access to your phone. However, this can only happen if your phone is within the Bluetooth range of a potential hacker. Usually, this range is around 30 feet. If the hacker successfully gets connected to your phone, the hacked phone will get exposed to all types of vulnerabilities related to its security.



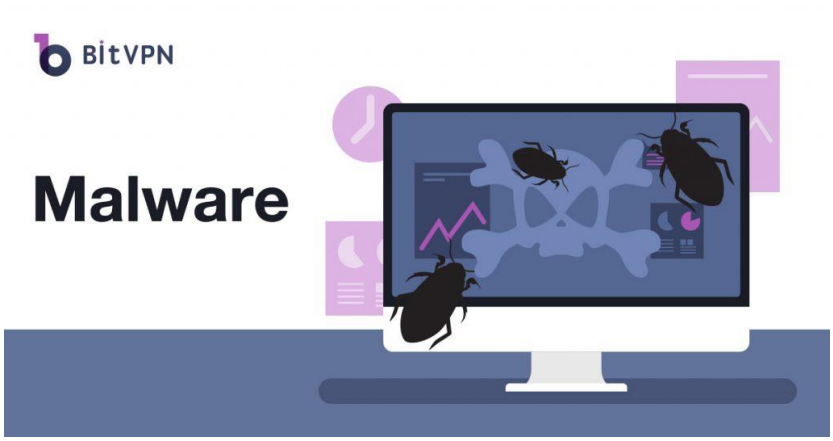
How Can Hackers Hack Into My Phone through Bluetooth?

Before we dig into how Bluetooth hackers hack into your phone. Let's recall how a Bluetooth connection occurs. First, you enable your Bluetooth function through settings on your phone. Then, select your target Bluetooth devices like headphones, speakers, etc. Now, you can successfully get connected with your target device with your phone. The process just takes a couple of seconds. In addition, as soon as you turn on your Bluetooth function on your cell phone, it also means your phone can be discovered by other devices within Bluetooth range. And that's the important part. It's that visibility that allows owners of nearby devices to get to your phone.

Hackers carry out Bluetooth hacks by setting up specialized software and hardware, through which they discover vulnerable devices equipped with active Bluetooth connections. This is done mostly in busy areas where hundreds of people congregate or commute on a regular

basis. Through the use of "professional" software and hardware, Bluetooth hackers can intercept a Bluetooth handshake – that's when two devices pair up and establish a connection – and use another encryption method to force their way into your device within a short time. Then, they will begin decrypting passwords and accessing other information almost instantly. The hacked device offers no indication or warning that it has been accessed by someone else. And the connection is lost as soon as the device goes out of range.

Bluetooth hacking is undoubtedly a serious security threat for billions of mobile phone users around the world. Several aspects of a phone can be controlled by this feature, including sending texts, making calls, transferring files, and displaying device information. Therefore, leveraging the "power" of this technology, Bluetooth hackers can easily jeopardize the online security of any unprotected device. Worse still, Bluetooth hackers can inject malware into your phone so that malicious code or viruses can be therefore transmitted from one device into another. That means that, because of the malware, the next attack can be implemented by someone even if he or she stays beyond the Bluetooth range.



How Can I Tell My Phone is Hacked by Someone through Bluetooth?

Although Bluetooth hacking occurs without your notice, you can still discover it through some signs on your phone.

Your phone's battery quickly goes down.

Although it's natural for a phone's battery life to go down as time goes by, it's a completely different thing when there's a reduction due to the attack by malware. It will be very abnormally obvious. Malware usually needs to scan the device and lots of battery has to be used to send information back to the server. Look out for rapidly falling battery life even when your device isn't being used. If this is happening, it would also be a sign that you have cryptomining malware installed on your device.

Your phone runs extremely slowly.

If your phone or installed applications often break down without any reason, your phone is possibly Bluetooth hacked. Malware overloads your phone's resources or arouses conflicts with other applications, which means they'll often just self-terminate. Or, you'll suffer from the constant running of some applications even though you try to quit them. And if you do manage to quit them, they still get restarted again and again.

Your phone uses high data.

If you suddenly get a huge bill for data usage, it probably derives from malware or spying applications that are sending huge quantities of your precious data back to the hacker's server.

Your phone receives text messages from strange numbers.

If you receive an SMS from a strange number, you must pay more attention because it possibly derives from malware distributing your number and forces your phone to pay for high-cost messaging.

Your phone has strange popups.

Strange popups always make you feel nervous although they don't definitely mean that your phone is hacked by someone. However, there's a basic principle to observe here: the more popups are there in your phone, the more probable it is your phone gets hacked. Therefore, when strange popups appear on your phone's screen, never click them unless you can be sure it'll be secure.

Any abnormality just occurs on your phone.

If your phone is hacked through Bluetooth, hackers can visit any of your accounts, from social media to email, from browsers to applications. All the accounts associated with those contain your private information: like passwords, credit card numbers, etc. Therefore, you should learn to be sensitive to abnormalities because any of them can be the result of hackers.

What's the Most Common Bluetooth Hacking?

A wireless technology, Bluetooth makes use of short-wavelength radio transmissions to exchange information within a short range of distance. However, this system comes with several flaws, making it vulnerable to hacking. Bluetooth-based attacks can be divided into the three categories below.

Bluejacking

This is the most common type of Bluetooth hacking. In these attacks, unsolicited messages

are sent by the hackers to discoverable Bluetooth devices in a specific area, utilizing the electronic business card feature of Bluetooth as the carrier. Bluejacking is relatively harmless in nature as the hacker can't intercept messages or access any information from the phone. They can still swamp you with explicit messages, though, which can be unpleasant.

Bluesnarfing

Much more serious in nature compared with Bluejacking, Bluesnarfing allows hackers to access certain personal information from the hacked phone. These attacks are carried out by using special software. Using this software, the hacker can send requests for access to information from a phone through the Bluetooth OBEX push profile. These attacks can be carried out invisibly.

Bluebugging

This type of attack can be much more powerful compared with Bluejacking and even Bluesnarfing. The hackers can gain complete control over a mobile device without the slightest clue to the owner of the device. However, this form of hacking is extremely difficult and is only feasible on older mobile phone models with outdated firmware.

How to Prevent My Phone from Bluetooth Hacking?

Many people tend to believe that hacking is not easy. Unfortunately, this is not true.

Also, please don't make the mistake of assuming that your phone won't be hacked because it has no valuable information. That's not true. Your identity may be illegally misused by hackers who steal your credit card number, email, or phone number. Therefore, you must protect your online privacy and security.

The following simple steps can be learned to protect your mobile devices from being hacked when you use Bluetooth:

Turn off Bluetooth and WiFi

If these features always remain 'on', the hackers can find out the networks you have frequently connected to and emulate them. Only turn on these features when you need to use them. A great way to protect your device when using WiFi is a VPN.

Use Two-Step Authentication

This is an excellent preventive measure because even if your password is accessed by someone, he or she can't login without physical access to your phone.

Create a Smart Password

Create a password with various numbers and characters placed sporadically. When it comes to a password of a bank account, it's understandable to avoid the same password for all accounts. However, in terms of a password for Bluetooth, most are more relaxing. Most people don't take their Bluetooth password seriously – if they even have one. It only contains four digits, for example, usually things like 1111, 0000, or 1234. They're too simple as passwords for hackers to defeat. Make a more difficult password that cannot be easily guessed.

Turn your Bluetooth setting to invisible mode, when not in use.

If you use Bluetooth when you drive, remember to turn it off before getting out of your car. If you are in a café or bar and don't need it, turn it off or to invisible. After all, your Bluetooth is most easily hacked in public.

Update the firmware of your devices regularly.

Never enter a PIN or link keys when prompted by unknown sources.

Stay away from open WiFi networks.

Well, you should know Bluetooth is not the only way for you to get hacked. As you get connected with internet, all your online activities will be monitored or exposed to all online hackers based on your IP address if you don't use a VPN. Most hacking occurs through your internet connection. VPN can protect your online security and privacy from your first click to the Internet.